actas da 6ª Conferência de Redes de Computadores – CRC2003, Bragança, Portugal, 29-30 Setembro de 2003

Controlo Transaccional em Sistemas de Gestão de Redes por Políticas

Vitor Roque
Instituto Politécnico da Guarda, ESTG, Guarda
vitor.roque@ipg.pt

José Luís Oliveira
Universidade de Aveiro, DET, Aveiro
jlo@det.ua.pt

Rui P. Lopes
Instituto Politécnico de Bragança, ESTiG, Bragança
rlopes@ipb.pt

Palavras chave: Gestão de Redes, Gestão de Redes por Políticas, Especificação de Políticas, Transacções.

Resumo

A gestão das redes tornou-se, nos últimos anos, um tema de máxima importância para as empresas dado que a sua organização, os fluxos de informação e métodos de trabalho, quer interna quer externamente, estão cada vez mais dependente do bom funcionamento de redes de comunicações. Esta dependência faz com que a *disponibilidade* e *desempenho* destas infra-estruturas e serviços sejam actualmente factores determinantes para o seu sucesso.

Tem-se assistido também a um aumento quer a nível de tamanho, quer a nível de complexidade das redes, o que implica o desenvolvimento rápido de mecanismos de configuração normalizados para que a sua gestão seja feita de uma forma eficaz e rápida. Espera-se que estes mecanismos estejam também fortemente ligados a sistemas de tolerância a falhas bem como a sistemas de gestão de desempenho.

O conceito de gestão por políticas surgiu nos últimos anos como o paradigma "ideal" para tratar este tipo de necessidades. As aplicações de gestão de rede por

políticas para configuração de rede em domínios administrativos podem ser bastante complexas a nível da própria estrutura, bem como devido aos relacionamentos possíveis de existir entre as suas partes constituintes. Apesar dos mecanismos de controlo transaccional terem vindo a ser relegados para plano secundário no âmbito da gestão de redes, a sua implementação assume um papel cada vez mais importante, nomeadamente no contexto de gestão baseada em políticas.

Neste artigo apresenta-se um mecanismo de controlo transaccional para sistemas de gestão de redes por políticas.

1. Introdução

As redes de comunicação tiveram um grande crescimento nos últimos anos. Este crescimento pode ser visto de diferentes perspectivas:

Escala – as redes possuem cada vez mais elementos, cada vez há maior diversidade de elementos e estes requerem cada vez mais recursos dos sistemas que os gerem.

Funcionalidade – os elementos de rede têm cada vez maior capacidade para desempenhar mais funções. Cada vez mais protocolos e níveis de rede são necessários para o desenvolvimento de novos serviços.

Intervalo de alteração – a natureza dos actuais serviços de rede requer intervalos de alteração (actualização, adição, remoção) da configuração da rede mais pequenos que num passado recente. Não é possível actualmente fazer-se a configuração da rede e pensar que a mesma se vai manter por muito tempo. Esta deverá ser alterada de acordo com as necessidades dos seus utilizadores.

Complexidade – devido à crescente complexidade dos equipamentos e respectiva gestão, novas tecnologias e novos serviços de rede, a gestão da rede é cada vez mais complexa.

Eficiência/Desempenho – novas tecnologias aplicadas a novos equipamentos de rede tornam as redes mais eficientes em termos de desempenho e fiabilidade.

Tendo em conta este conjunto de problemas e requisitos, urge definir mecanismos de configuração normalizados de forma a garantir uma gestão homogénea dos diferentes equipamentos que fazem parte de uma rede. Uma possível resposta a este problema é a Gestão de Redes por Políticas *(PBNM – Policy-Based Network Management)*. Os sistemas PBNM vão permitir que a configuração da rede seja feita de uma forma "automática" com base em regras de alto-nível [1]. Por exemplo, o sistema de gestão deverá ser capaz de, para uma determinada situação, oferecer facilidades para reconfiguração do sistema na sua totalidade, se necessário, sem que o gestor da rede tenha que se preocupar com os detalhes de configuração dos diferentes equipamentos que constituem a rede.

Tendo em conta que as tarefas de configuração podem ser demoradas, isto é, levar muito tempo até que as mesmas sejam completadas, haver longos períodos de inactividade, além da complexidade inerente aos relacionamentos entre os diferentes elementos constituintes da rede, os sistemas PBNM devem oferecer suporte para tolerância a falhas, pois a segurança/confiança na integridade transaccional a nível do protocolo é insuficiente.

Uma técnica comum para suporte de tolerância a falhas é através da utilização de transacções atómicas com suporte das propriedades *atomicidade*, *consistência*,

isolamento e *durabilidade* também conhecidas como ACID, conseguindo-se desta forma assegurar trocas de estado consistentes apesar de possíveis acessos concorrenciais e falhas [2].

Neste artigo discutir-se-á o conceito de gestão baseada em políticas e da relevância de descrever e implementar operações de gestão consistentes. No seguimento apresentar-se-á uma proposta de controlo transaccional num modelo de políticas bem como a sua aplicação em protocolos de gestão actuais.

2. Gestão de Redes e Políticas

Os sistemas de gestão tradicionais estão muito relacionados com aspectos de instrumentação de baixo nível e até há pouco tempo a gestão por políticas (regras de alto-nível) não estava regulamentada/normalizada.

O esforço de normalização da gestão por políticas parte principalmente de organizações como o IETF e o DMTF resultando propostas como: COPS [3] e SNMP *for Configuration* [4], CIM [5] e PCIM [6].

Estes desenvolvimentos conduziram à definição de uma arquitectura para uma *framework* de políticas composta por quatro entidades funcionais (Figura 1) [7]: a *Policy Management Tool – Policy Console*, o *Policy Repository*, o *Policy Decision Point (PDP)* e os *Policy Enforcement Points (PEP)*. Este modelo descreve os componentes chave mas não faz qualquer referência a detalhes de implementação como por exemplo distribuição, plataforma ou linguagem. Como consequência, a *Policy Console* é de todos os componentes o menos definido e as suas funcionalidades dependem grandemente das opções assumidas pelos programadores.

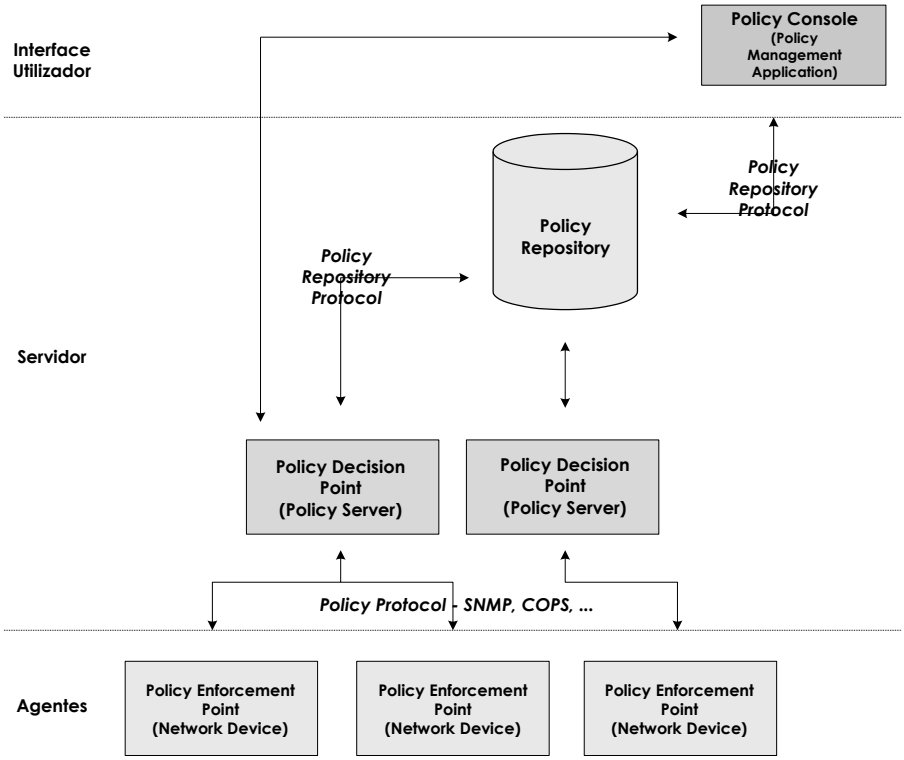

Figura 1 – Gestão de Redes baseada em Políticas: Modelo conceptual.

O PDP é a entidade responsável pela verificação de quando e como as políticas podem ser aplicadas. Valida as decisões com base em medições de tráfego, análise da

contabilidade, perfis de utilizadores, detecção de eventos e trata também da determinação e validação de aplicabilidade de regras a nível de recursos específicos e funções de adaptação dos dispositivos.

O termo "política" neste contexto tem o seguinte significado: uma ou mais regras que descrevem as acções a ser realizadas quando determinadas condições se verificam. Semanticamente pode ser expressa como [8]:

if (policyCondition) then (policyAction)

Do outro lado, o PEP é o elemento onde as decisões são aplicadas quando as condições devolvem o valor lógico "verdade". São os responsáveis pela execução das acções podendo realizar operações adicionais como a verificação e a validação de condições. Como exemplos de PEP's temos routers, switches, firewalls, proxies, genericamente qualquer entidade passível de ser gerida.

O *Policy Repository* é o local onde toda a informação relacionada com políticas é guardada. A informação aqui guardada descreve, entre outra informação, utilizadores autorizados, aplicações, computadores e serviços e os seus relacionamentos.

Um protocolo apropriado (COPS, SNMP, ...) é utilizado para a transferência de informação de políticas entre PDP's e entre PDP's e PEP's.

Políticas e Regras

Como definido anteriormente, política é uma ou mais regras que descrevem as acções a ocorrer quando determinadas condições se verificam. As políticas podem ser simples ou resultarem da composição de duas ou mais regras ou mesmo da composição de várias políticas (política de políticas). As regras são os elementos mais simples (atómicos) que constituem as políticas.

Regras simples, são regras que são constituídas por duas expressões lógicas binárias. A primeira define o domínio de aplicabilidade da regra e a segunda o domínio de aceitabilidade da regra.

Regras compostas, são regras resultantes da composição de regras simples ou regras compostas. As operações que podem ser utilizadas na composição de regras são a conjunção *(and)*, disjunção *(or)* e negação *(not)*. A definição de políticas simples e compostas é idêntica à definição de regras simples e compostas, isto é, uma política composta é o resultado da composição de políticas simples ou compostas (Figura 2).

If (direction is out)
  If (protocol is UDP) THEN (guarantee 30% of available BW)
  If (protocol is TCP) THEN (guarantee 40% of available BW)

} *Política composta*

Quer em regras compostas, quer em políticas compostas, as regras ou políticas não devem entrar em conflito umas com as outras. Não deve ser possível, por exemplo, ter políticas a autorizar o acesso a um recurso e outra, na mesma política geral, a negar o acesso a esse mesmo recurso.

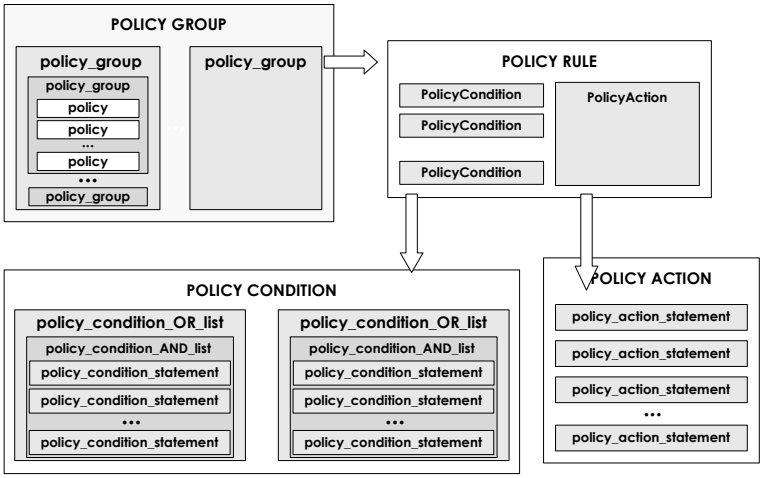

Figura 2 – Relacionamento entre políticas, condições, acções e grupos.

3. Políticas e Transacções

A gestão de redes por políticas é uma metodologia em que a informação de configuração é obtida a partir de regras e objectivos de funcionamento da rede sendo a mesma distribuída por vários elementos de rede com o objectivo de no final se conseguir um comportamento consistente da rede.

A actividade de configuração, aplicação das políticas, provoca alterações de estado nos elementos de rede e é crítico que o sistema manipule as alterações de configuração de forma atómica para que na troca de estado se passe de um estado consistente para outro estado consistente. O objectivo é que a alteração de configuração nos diferentes elementos de rede num domínio administrativo se faça como um todo, ou na impossibilidade de tal acontecer seja reposta a configuração anterior, mesmo que em alguns elementos a instalação da nova configuração tenha tido sucesso (Figura 3).

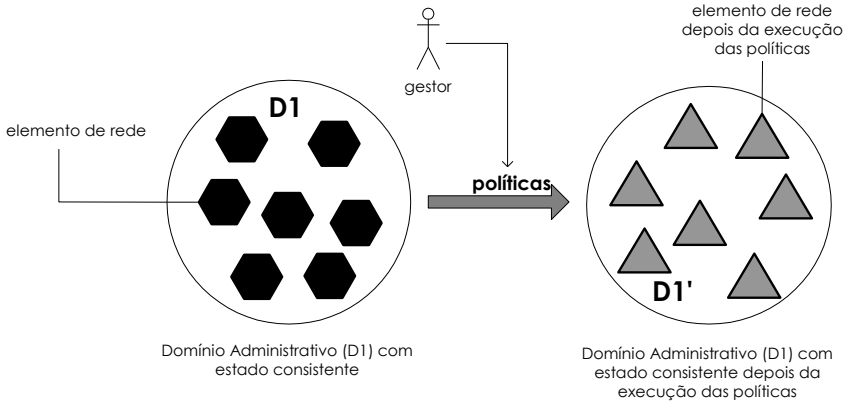

Figura 3 – Passagem de um estado consistente a outro estado consistente num domínio administrativo.

Se se considerar a associação política – transacção, isto é, considerar-se uma política como uma transacção, em que todas as operações (regras – condição/acção) têm que ser executadas ou nenhuma operação é executada, no caso de haver uma operação que falhe toda a instrução de configuração deve ser abortada. Devido a esta situação, os sistemas de gestão de redes por políticas devem implementar as propriedades ACID, isto é, as aplicações devem ter a capacidade de monitorizar as operações realizadas nos objectos dos elementos de rede e o início e o fim da aplicação da regra/transacção. Se

uma operação a realizar sobre um objecto puser em causa alguma destas propriedades o sistema deve ter a capacidade de retornar ao estado anterior.

4. Um Mecanismo para Controlo Transaccional

A definição de um mecanismo para controlo transaccional em sistemas de gestão de redes por políticas é fundamental pois a segurança/confiança na integridade transaccional a nível do protocolo é insuficiente [4].

O mecanismo proposto utiliza os conceitos de servidor (PDP) e agente (PEP) do modelo de políticas. A comunicação é unidireccional, no sentido PDP – PEP dado que a gestão é feita de forma centralizada no PDP e será este a ter a responsabilidade de questionar os PEP's relativamente à instalação das políticas.

Neste mecanismo o processo de configuração é baseado em cinco comandos:

- ***analisar*** *(PEP -> PEP)* – o agente efectua as operações relacionadas com as políticas sem no entanto as aplicar;
- ***testar*** *(PDP -> PEP)* – este comando é emitido pelo servidor para perguntar ao agente se o comando *analisar* teve sucesso.
- ***executar*** *(PDP -> PEP)* – é indicado ao agente que deve aplicar as operações assinaladas no comando *analisar*;
- ***retroceder*** *(PDP -> PEP)* – no caso de ocorrer algum erro, este comando é emitido pelo servidor para indicar ao agente que deve desfazer as alterações resultantes do comando *analisar*;
- ***limpar*** *(PDP -> PEP)* – será emitido pelo servidor para indicar ao agente que pode libertar os recursos utilizados durante a operação.

A utilização destes comandos permite garantir controlo transaccional a nível de políticas.

Este mecanismo funcionaria da seguinte forma: suponha-se que se pretende fazer a instalação de políticas nos elementos de rede de um determinado domínio administrativo como exemplificado pela Figura 4.

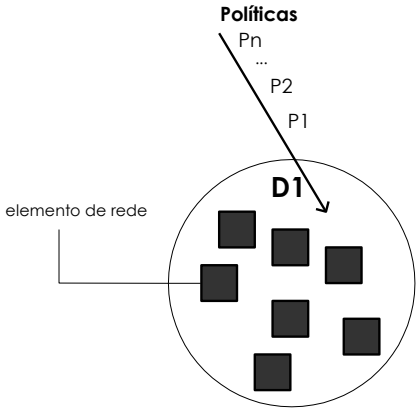

Figura 4 – Exemplo de instalação de políticas.

Uma vez que o PDP é o elemento centralizador da distribuição das políticas, os PEP's (agentes) devem estar num estado de escuta, à espera de serem contactados pelo servidor. Assim que o servidor os contacta, estes ficam à espera que o mesmo servidor

lhes envie a informação de configuração (políticas). A informação de configuração que o servidor vai enviar, são ficheiros de alto nível descritos em Extensible Markup Language (XML) e que são traduzidos de acordo com a linguagem e protocolo utilizado do lado do PEP. Tudo isto é tarefa do servidor (PDP) e é independente do mecanismo de controlo transaccional. As políticas são enviadas para os diferentes agentes – comando *analisar* – verificando o agente de cada elemento de rede se estas podem ser instaladas. No caso de não haver qualquer incompatibilidade é executado o comando *testar* em todos os agentes para verificação se o comando *analisar* teve sucesso. Este processo repete-se em todos os agentes dos diferentes PEP's do mesmo domínio administrativo. Na fase seguinte, o servidor (PDP) solicita a todos os agentes (PEP's), comando *executar*, a instalação efectiva da política. Se a resposta ao comando *testar* foi afirmativa por parte de todos os agentes o servidor emite o comando *limpar* para que os agentes libertam os recursos utilizados durante as operações. No caso de haver de algum dos agentes uma ou mais respostas de insucesso no comando *testar*, o servidor emite o comando *retroceder* para que seja reposta a configuração anterior nos PEP's. De imediato deverá emitir o comando *limpar* para que os agentes libertem os recursos utilizados durante as operações.

Na Figura 5 é representado na forma de diagrama de fluxos o mecanismo desenvolvido.

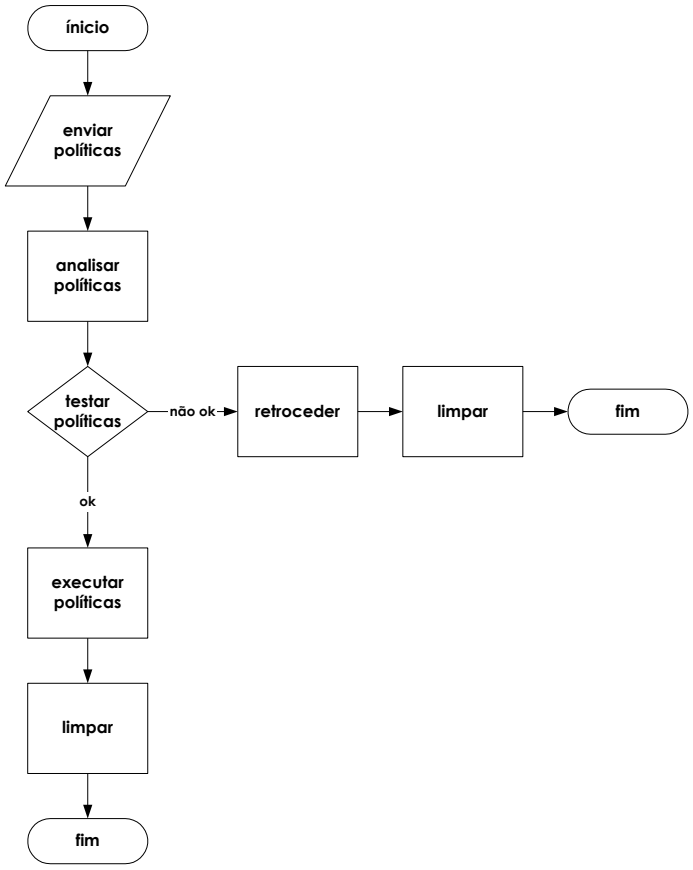

Figura 5 – Diagrama de fluxos do funcionamento do mecanismo transaccional.

Com a utilização deste mecanismo pretende-se especificar e activar o controlo transaccional de políticas entre diversos PEP's. O controlo transaccional de políticas entre PDP e PEP pode ser assegurado, caso exista, pelo mecanismo transaccional do protocolo utilizado.

Como protocolos utilizados no transporte de informação entre PDP's e PEP's destacam-se dois, nomeadamente o protocolo COPS desenvolvido especificamente para esta situação, nos modelos *Outsourcing* e *Configuration*, e o protocolo SNMP, como o protocolo mais utilizado na gestão de redes.

COPS

O protocolo COPS é um protocolo pergunta/resposta que suporta dois modelos para controlo de políticas: o modelo *Outsourcing* e o modelo *Configuration*, também conhecido como modelo *Provisioning*.

No modelo *Outsourcing* os eventos ocorridos no PEP requerem decisões imediatas que deverão ser tomadas pelo PDP – o PEP delega-lhe a responsabilidade decisória. No modelo *Provisioning* este relacionamento de um para um, entre eventos no PEP eventos e decisões no PDP, não se verifica. Neste, a transferência de informação pode ser feita em bloco, por exemplo pode ser descarregada a totalidade da informação de configuração QoS de um router, ou por partes, por exemplo a actualização de um filtro de marcação DiffServ, com espaçamento no tempo.

Os recursos de rede são frequentemente configurados de acordo com parâmetros de rede cuja variação é relativamente pequena. Enquanto o modelo *Outsourcing* está intimamente ligado à dinâmica tempo-real do PEP, o modelo *Provisioning* está essencialmente dependente do PDP sem grandes preocupações no que respeita a respostas imediatas.

Os dois modelos apresentam desta forma conceitos de funcionamento diferentes um do outro.

A tolerância a falhas em COPS é assegurada através da verificação em permanência da ligação PEP – PDP por intermédio do envio de mensagens *keep alive* [3]. Quando é detectada uma falha na ligação devido a uma condição de *timeout*, o PEP deve tentar estabelecer novamente a ligação com o PDP ou no caso de impossibilidade tentar a ligação com um PDP alternativo de acordo com os seus dados de configuração. Note-se que em COPS a responsabilidade de iniciar a ligação persistente é do PEP.

No caso de o PEP se encontrar ligado a um PDP alternativo e o PDP principal voltar a estar disponível, será da responsabilidade do PDP alternativo o redireccionamento do PEP para o PDP principal.

No caso de não ser possível a ligação do PEP a nenhum PDP, é da responsabilidade do PEP tomar as suas próprias decisões. No entanto, logo que a ligação seja restabelecida o PEP deverá informar o PDP de todas as alterações efectuadas na ausência de comunicação para que este possa solicitar a ressincronização de estados/comportamentos entre PEP's.

No caso de utilização deste protocolo para transporte de informação (políticas) entre PDP e PEP's, o mecanismo de tolerência a falhas disponibilizado pelo conjunto e sequência das mensagens trocadas é suficiente para garantir o controlo transaccional a nível das políticas. No entanto o mapeamento do mecanismo desenvolvido, para este protocolo, devido à diversidade de mensagens e objectos disponibilizados [3, 9], é simples.

SNMP

O protocolo SNMP consiste num protocolo que permite verificar e modificar a informação de gestão de um elemento remoto de rede (agente), bem como o transporte de notificações geradas por estes (traps) [10].

Se pretendermos utilizar SNMP como protocolo de transporte de políticas entre PDP e diversos PEP's, devemos garantir o controlo transaccional ao nível das políticas, mapeando cada política em comandos do próprio protocolo e acções no agente. O tamanho de mensagem do protocolo SNMP revela-se um inconveniente pois unicamente são permitidas pequenas actualizações atómicas, podendo a instalação completa da política levar demasiado tempo, provocando desta forma inconsistência da própria política, isto é, as primeiras actualizações já não estarem de acordo com actualizações posteriores. Uma outra possível consequência é que o tamanho de mensagem pode não comportar uma linha completa de uma tabela de uma MIB. Desta forma o preenchimento de uma linha na totalidade, numa tabela, pode necessitar mais de uma mensagem, o que pode acarretar problemas de consistência ao nível da própria linha, por desfazamento temporal da informação.

Com o objectivo de normalização da distribuição de políticas, o grupo de trabalho *Configuration Management with SNMP (snmpconf)* do IETF definiu uma Management Information Base (MIB) para políticas, a *Policy Based Management MIB* [11], que contém um conjunto de objectos relacionados com políticas que podem ser monitorizados (verificação e modificação).

5. Editor Visual de Políticas e Transacções

O objectivo de desenvolvimento deste mecanismo prende-se com trabalho realizado anteriormente, nomeadamente a construção de um protótipo para especificação de políticas de forma gráfica (GUI) [12].

Com o desenvolvimento deste mecanismo, vamos poder dotar o editor gráfico de políticas com controlo transaccional, isto é, disponibilização de interfaces do mecanismo transaccional para serem utilizadas pela aplicação (editor gráfico de políticas), mantendo desta forma a separação aplicação – mecanismo.

O editor de políticas permite ao utilizador a definição de políticas através de uma única linguagem de especificação, XML, sendo que a informação resultante é transferida para os elementos de rede com recurso a uma única sintaxe. Os ícones utilizados no editor, para a especificação das políticas, são dinamicamente gerados com base em esquemas XML.

As políticas devem seguir as especificações definidas num *template* normalizado (DTD/Schema) onde é referida toda a informação relevante que a mesma deve possuir. Depois de validada, a política deve ser enviada para os elementos de rede Figura 6. No caso dos elementos de rede (agentes), serem compatíveis XML, a política é entregue directamente, no caso dos elementos de rede não suportarem a norma XML então a política deverá primeiro passar por um conversor, que transformará a linguagem XML (política) numa linguagem específica própria do elemento de rede.

Depois de recebidas as políticas por parte dos elementos de rede (agentes) o mecanismo transaccional apresentado anteriormente garante que as políticas recebidas pelos agentes são tratadas de acordo com as propriedades ACID.

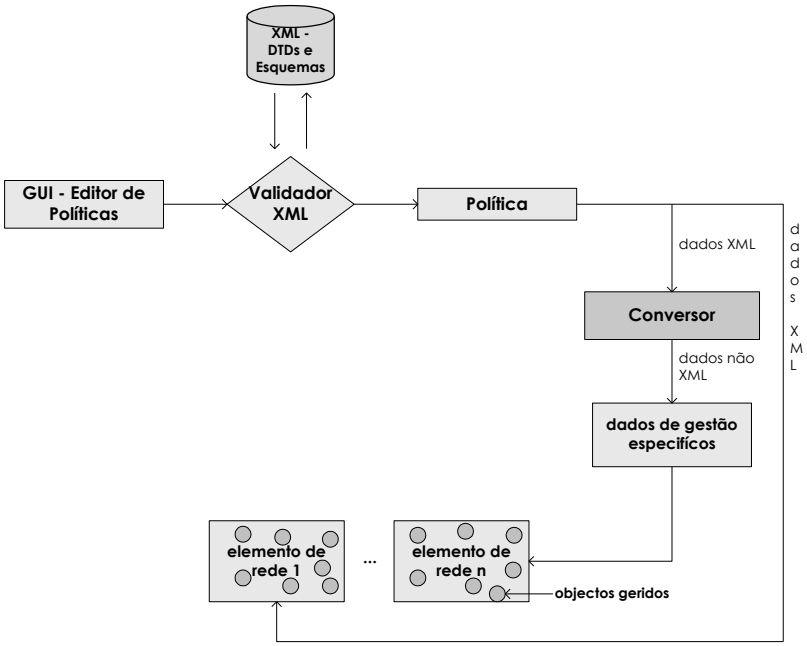

Figura 6 – Modelo XML para políticas.

6. Conclusões

A gestão por políticas é uma metodologia em que a informação de configuração é especificada segundo regras e objectivos que depois de distribuídos pelos diferentes elementos de rede irão assegurar um comportamento consistente num domínio administrativo.

Uma vez que as actividades de configuração provocam alterações de estado nos diferentes elementos de rede é fundamental que o sistema em causa trate as alterações de configuração de forma atómica.

O desenvolvimento de um mecanismo transaccional para gestão da instalação de políticas nos diferentes elementos de rede, prende-se com o facto de no trabalho que vem sendo desenvolvido nos termos deparado com lacunas ao nível dos modelos de gestão actuais – este trabalho é deixado a cargo dos sistemas centrais de gestão que terão de tratar, caso a caso, a sua implementação.

Neste artigo foram feitas algumas considerações relativamente à relevância de existirem mecanismos transaccionais ao nível da especificação de políticas de gestão e apresentadas algumas soluções que podem ser utilizadas nos sistemas actuais. Na definição deste mecanismo partimos do pressuposto que a semântica *commit/rollback* de transacções ACID é suficiente. De acordo com esta suposição, mesmo na presença de falhas, a transição de estado de forma consistente dos elementos de rede é garantida.

7. Referências bibliográficas

1. Sloman, M., *Policy driven management for distributed systems.* Journal of Management Information Systems, 1994. **2**(4): p. 333-360.
2. Date, C.J., *An Introduction to Database Systems: International Edition*. 1999: Addison Wesley.

3. Durham, D., et al., *The COPS (Common Open Policy Service) Protocol - RFC2748*. 2000, IETF.
4. MacFaden, M., et al., *Configuring Networks and Devices With SNMP - RFC3512*. 2003, IETF.
5. *CIM-Core, Common Information Model - Core Model v2.6*. 2002, DMTF.
6. Moore, B., et al., *Policy Core Information Model Specification v1 - RFC3060*. 2001, IETF.
7. Kosiur, D., *Understanding Policy-Based Networking*. 2001: Wiley.
8. Westerinen, A., et al., *Terminology for Policy-Based Management - RFC3198*. 2001, IETF.
9. Chan, K., et al., *COPS Usage for Policy Provisioning (COPS-PR)*. 2001, IETF.
10. Stallings, W., *SNMP, SNMPv2, and RMON 1 and 2*. 3rd ed. 1999: Addison Wesley.
11. Waldbusser, S., J. Saperia, and T. Hongal, *Policy Based Management MIB*. 2003, IETF.
12. Roque, V., J. Oliveira, and R. Lopes. *Visual Composition of Management Policies*. in *4th Conference on Telecommunications (ConfTele2003)*. 2003. Aveiro - PORTUGAL.